UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

MINERAL AREA COMMUNITY PSYCHIATRIC REHABILITATION CENTER, INC.,	)	
Plaintiff,	)	
vs.	)	**Case No. 4:20-CV-1427 PLC**
KYLE L. DUNCAN,	)	
Defendant.	)	

MEMORANDUM AND ORDER

This matter is before the Court on Defendant Kyle Duncan's motion to dismiss the complaint for failure to state a cause of action pursuant to Fed. R. Civ. P. 12(b)(6). [ECF No. 5] Plaintiff Mineral Area Community Psychiatric Rehabilitation Center, Inc. opposes the motion. [ECF No. 7]

Plaintiff filed a three-count complaint against Defendant, its former employee, alleging: (1) violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030; (2) replevin; and (3) violation of the Missouri Computer Tampering Act, Mo. Rev. Stat. § 537.525. In support of its claim under the CFAA, Plaintiff alleges that, prior to Defendant's termination, Defendant used his employer-provided laptop to access and send Plaintiff's confidential documents to his private email account. [ECF No. 1] Plaintiff states that Defendant's "access to Plaintiff's computers was without authorization and/or exceeded authorization[.]" [Id.]

In his motion to dismiss, Defendant moves the Court to: (1) dismiss Plaintiff's CFAA claim for failure to state a cause of action pursuant to Fed. R. Civ. P. 12(b)(6); and (2) decline to exercise supplemental jurisdiction over Plaintiff's remaining state law claims. [ECF Nos. 5 & 6]

To survive a motion to dismiss pursuant to Rule 12(b)96), "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim for relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id.

The CFAA creates criminal and civil liability for a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer." 18 U.S.C. §§ 1030(a)(2)(C), 1030(g). The CFAA provides that "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

Defendant argues that Plaintiff failed to state a claim for relief under the CFAA because Defendant was authorized to use the laptop computer and access the information he allegedly obtained. [ECF No. 6] Citing the Ninth Circuit's decision in United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016), Defendant argues that the statutory term "exceeds authorized access" does not extend to violations of a company's use restrictions.

In response, Plaintiff asserts that it pleaded sufficient facts to state a claim under the CFAA when it alleged that Defendant "was without authorization or exceeded his authority when he deliberately accessed and sent confidential information to his personal email address from his company computer." [ECF No. 7 at 3] In support of its position, Plaintiff cites three cases from the Eastern District of Missouri in which the court found that the plaintiffs stated claims under the CFAA when they alleged that former employees acted "without authorization" after they breached their duties of loyalty. See Bayer, U.S., LLC v. Zeng, No. 4:20-CV-431 SRC, 2020 WL 4429542

(E.D. Mo. July 31, 2020); Pinebrook Holdings, LLC v. Narup, No. 4:19-CV-1562 RLW, 2020 WL 871578 (E.D. Mo. Feb. 21, 2020); Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg. & Consulting, LLC, No. 4:08-CV-1683 JCH, 2009 WL 3523986 (E.D. Mo. Oct. 26, 2009). As Defendant points out in his reply, however, the cases cited by Plaintiff did not involve challenges to the meaning of "exceed authorized access" under the CFAA.

The question Defendant raises in his motion to dismiss – specifically, whether an employee violates the CFAA when he accesses an employer's information, which he has permission to access, but with an improper purpose – is the subject of a split among the circuit courts of appeal. See Nosal, 844 F.3d at 1033-34 (discussing circuit split); Porters Bldg. Ctrs., Inc. v. Sprint Lumber, No. 16-6055-CV-SJ-ODS, 2017 WL 4413288, at *2 (W.D. Mo. Oct. 2, 2017) (same); Integrated Process Sols., Inc. v. Lanix LLC, No. 19-CV-567 NEB/LIB, 2019 WL 1238835, at *5 (D. Minn. Mar. 18, 2019) (same). The Eighth Circuit has not addressed this issue. See, e.g., Integrated Process Sols., 2019 WL 1238835, at *5 ("The Eighth Circuit has not commented on this split[.]"); TripleTree, LLC v. Walcker, No. 16-609 DSD/TNL, 2016 WL 2621954, at *3 (D. Minn. May 6, 2016) ("The Eighth Circuit has not determined whether the CFAA imposes civil liability on employees who access information with permission, but with an improper purpose.").

The majority, or narrow, view, which Defendant urges the Court to adopt, holds that employees exceed authorized access when "they use a computer or obtain information they do not have authority to use or obtain – not when they merely misuse information they had proper authority to access." Integrated Process Sols., Inc., 2019 WL 1238835, at *5. See Facebook Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067-68 (9th Cir. 2016); Hunn v. Dan Wilson Homes, Inc., 789 F.3d 573, 583-84 (5th Cir. 2015); United States v. Valle, 807 F.3d 508, 527-28 (2d Cir. 2015); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 203-07 (4th Cir. 2012).

According to the majority interpretation of the CFAA, "the misuse or misappropriation of confidential information stored on a computer to which the defendant has authority to access does not give rise to liability."[1] Sebrite Agency, Inc. v. Platt, 884 F.Supp.2d 912, 917 (D. Minn. 2012).

The minority, or broad, reading of the CFAA, which Plaintiff espouses, provides that an employee acts without or exceeds authorization when he or she "us[es] or access[es] data for purpose contrary to the reason for which the authorization was originally given."[2] InfoDeli, LLC v. Western Robidoux, Inc., No. 4:15-CV-364-BCW, 2020 WL 1866001, at *5 (W.D. Mo. Feb. 28, 2020). See Pulte Holmes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 303-04 (6th Cir. 2011); United States v. Rodriguez, 628 F.3d 1258, 1263-64 (11th Cir. 2010); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 421 (7th Cir. 2006); P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore LLC, 428 F.3d 504, 510-11 (3d Cir. 2005). The minority view therefore deems the CFAA to "cover actions by an employee who, although given access to an employer's computers, utilizes information from the computers for personal use, in contravention of the employee's duty of loyalty, or to aid unlawful competition." Porters Bldg. Ctrs., 2017 WL 4413288, at *2.

---

[1] The courts taking the narrow (majority) view of the CFAA reason that "the plain language of the CFAA target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation." Nosal, 844 F.3d at 1034 (alterations in original) (quotation omitted). See also GPMM, Inc. v. Tharp, No. 8:19-CV-128, 2019 WL 7161229, at *5 (D. Neb. Oct. 3, 2019) ("The CFAA is clear that authorization extends only to the *access* and not the *use* of information as prohibited conduct. Therefore, it matters to what extent an employer granted an employee access to a computer system, not what prohibitions the employer put on the employee's use of information obtained therefrom.") (emphasis in original) (internal citation and parenthetical omitted). The Ninth Circuit explained that, under this interpretation, "'[w]ithout authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorization access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files." Nosal, 844 F.3d at 1034 (alterations and emphasis in original) (quotation omitted).

[2] The Western District of Missouri has adopted the broad (minority) interpretation of the CFAA's meaning of without or exceeding authorization. See InfoDeli, LLC, 2020 WL 1866001, at *5; Porters Bldg. Ctrs., 2017 WL 4413288, at *2-3.

Importantly, although not raised by either party, the United States Supreme Court is set to resolve the question of whether an individual who is authorized to access information on a computer for certain purposes violates the CFAA when he accesses the same information for an improper purpose. United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019), cert. granted, 140 S. Ct. 2667 (2020).[3] The Supreme Court's decision in Van Buren, which may be expected within the next year, will therefore determine whether Plaintiff presents a viable claim for the unauthorized access of its confidential information under the CFAA.

In light of the petition for certiorari pending before the Supreme Court in Van Buren, the Court questions the efficiency and usefulness of deciding the instant motion to dismiss before the Supreme Court issues its decision. This Court has "inherent power" to grant a stay "in order to control its docket, conserve judicial resources, and provide for a just determination of the cases pending before it." Contracting Nw., Inc. v. City of Fredericksburg, 713 F.2d 382, 387 (8th Cir. 1983). Whether to grant a stay "calls for the exercise of judgment" where courts must "weigh competing interests and maintain an even balance." Landis v. N. Am. Co., 299 U.S. 248, 254–55 (1936). "Specifically, this Court weighs 'potential prejudice or hardship to the parties, as well as the interest of judicial economy.'" Seefeldt v. Entm't Consulting Int'l, LLC, No. 4:19-CV-188 MTS, 2020 WL 4922371, at *1 (E.D. Mo. Aug. 21, 2020) (quoting St. Louis Heart Ctr., Inc. v. Athenahealth, Inc., 4:15-cv-01215-AGF, 2015 WL 6777873, at *5 (E.D. Mo. Nov. 4, 2015); see also Barkley v. Woodbury Cnty., Iowa, 874 F.Supp.2d 759, 764 (N.D. Iowa May 23, 2012) (court previously entered an order sua sponte staying case until the Supreme Court issued decision).

[3] In Van Buren, the defendant police officer searched a police database for a license plate number in furtherance of his efforts to bribe a citizen for money, and a jury found him guilty of felony computer fraud under the CFAA. 940 F.3d at 1197-98. On appeal, the Eleventh Circuit reaffirmed its earlier holding that "even a person with authority to access a computer can be guilty of computer fraud [under the CFAA] if that person subsequently misuses the computer." Id. at 1207-08 (citing Rodriguez, 628 F.3d at 1263).

Accordingly,

IT IS HEREBY ORDERED that the parties submit to the Court **within seven days after the date of this order** briefs explaining why deciding the instant motion to dismiss is a reasonable use of judicial resources and why this case should not be stayed pending the Supreme Court's decision in Van Buren.

Patricia L. Cohen

PATRICIA L. COHEN
UNITED STATES MAGISTRATE JUDGE

Dated this 11th day of January, 2021